DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

20 March 1982
DCISEC-CSS-M145

1. The One Hundred and Forty-Fifth meeting of the Computer Security
Subcommittee was held on 16 March 1981 at [   ] McLean,
VA. The meeting was convened at 0930, and attending were:

[   ] Chairman
[   ] Executive Secretary
[   ] CIA
[   ] CIA
[   ] CIA
Mr. Robert Graytock, Dept. of Justice
Mr. David Schenken, U.S. Secret Service
Mr. Carl Martz, Navy
LtC. William Chantelau, Army
Mr. William Condon, Dept. of State
Mr. Robert Storck, FBI
Mr. Gene Epperly, OSD

2. The Chairman opened the meeting with a review of the progress of
the two CSS-funded tasks at Los Alamos (i.e, Technology Forecast and
Evaluation of the Wang 250 Word Processor). The Statements of Work (SOW)
were substantially revised and considerably more detail added, NSA revising
the SOW on the Technology Forecast task, and CIA revising that of the Word
Processor task. The funds to cover these tasks ($200K) have already been
transferred to the Los Alamos National Laboratories. The remaining portion
($50K) of CSS's original allocation is being withheld as part of a budget
hold on SECOM funds. There appears to be little chance, at this time, that
the remaining funds will be restored. The Chairman reported that he has
requested an additional $250K for fy 83, and $500K for fy 84. He requested
that the membership give some thought to what projects they would propose
the CSS fund for fy 83, and be prepared to present these by June. Detailed
proposals are not required at that time, but basic project ideas should be
presented. He stated that he would like to start discussions for
disposition of the fy 84 funds by late summer. He noted that the fy 83
funds apear firm at this point in time.

3. The primary topic of this meeting was the draft DCID 1/16. The
major points of these discussions were as follows;

   a. Army – Objected to the switch in definitions (i.e., the use of
the term "multi", as in multi-compartmented, to mean more than one
participating NFIB agency, rather than more than one compartment of data)
as being unnecessarily confusing. It was pointed out later that the
problem is more basic than just a change in meaning of a word, the approach
taken in the draft actually changes the basis for making decisions from the
mix of classification levels and compartments to the number of
participating agencies and departments.

g. OSD - Mr. Epperly pointed out, as discussed above, that the basis for definition of modes has been changed by the proposed DCID, and asked if the cost for doing this was worth the cost. Basically, he felt that it has taken a considerable period of time for the field to become familiar with the present modes, their meaning and impact, and that changing the basic definitions now would cause considerable confusion.

STAT

h. DIA - also voiced objection to the change in definitions, and therefore in the basis for decision-making. Noted that the absence of the existing collateral mode was not acceptable. Further observed that the present draft does not include a section on minimum standards for personnel security, physical security, hardware/software, etc. [   ] felt most strongly about two points in particular. First, that there needs to be more flexibility in the ability to engineer operational systems; he stated that his desires were more in line with the approach first outlined by Mrs. Mathieu (NSA), incorporating a broad policy statement along with an implementing regulation which did not overly and unnecessarily restrain the operational elements. Secondly, that there needs to be a networking section; the future will be networks tying together word processors, communications front ends, and user support systems, and it is essential that the DCID articulate the basic security requirements which support the security-related decision concerning which networks are acceptable for passing intelligence community information.

i. There was a lengthy discussion of the networking issue, mostly centered about the types of statements that the DCID should make on this subject. It was generally agreed that the document should address security requirements for networking (.e.g., misrouting protection, anti-spoofing, etc.), and most definitely not attempt to dictate communications technology to be implemented, system architecture, or specific mechanisms for achieving the desired protection. That is, ideally, the document would specify the types of protection required and not how the requirements will be satisfied. DIA distributed a recent DIA paper, "DoDIIS Network Security Models" (copy attached) for the consideration of the members, and as a potential aid in developing the desired wording for the networking section. It was agreed that the NSA member would prepare a draft for the networking section for the next meeting, although any other member is also invited to propose wording for this section.

j. The chairman re-emphasized the fact that the expressed wishes of the DCI are for DCID's which articulate policy only, leaving implementation to the individual NFIB member agencies. He also pointed out that any changes to a DCID must be handled through the NFIB, which can be a long and laborious process, whereas changes to an accompanying regulation can be made at a lower level, and therefore much quicker. Thus, he felt that there were some practical advantages to publishing a relatively stable, long-lived, broad statement of policy, to which is coupled a more dynamic implementing regulation.

b. FBI - expressed a preference for a more liberal approach to systems engineering, allowing individual KFIB agencies to engineer systems according to the specific needs and environment, rather than being constrained by a fixed number of pre-ordained modes. He also expressed approval of the mechanism for allowing new modes to be proposed, reviewed, and approved.

c. Dept. of Justice - basically satisfied with the approach taken by the draft DCID.

d. At this point there was a discussion of the scope of the policy; there apparently exists conflict/overlap between the DCID and the Executive Order on collateral, or non-SCI, foreign intelligence. The Chairman will raise this flag to the SECOM. There was a recommendation by the Navy member to limit the scope of DCID 1/16 to SCI only. It was brought out in the ensuing discussion that such a step would have the effect of exempting all HUMINT and counter-intelligence data, since these are not SCI categories. For an agency such as the FBI, most of whose sensitive information falls into this class of data, this would cause a major problem in that the DCID would provide no authority to govern internal ADP operations. That is, if there is, in effect, no policy, then it becomes difficult to enforce authority and ensure that adequate protection mechanisms are employed. No decision was reached on the question of the scope of the policy definition, although a query by the chairman revealed that the Navy member was the only member present who had strong feelings on this issue. It was agreed that the existing regulatory documents would need to be reviewed for definitions of what is, and is not, foreign intelligence, and where the authority lies for defining handling/protection policy.

e. CIA - felt that the "boiler-plate" requirements section is necessary and that the present draft allows sufficient flexibility by incorporating a mechanism for individual agencies to propose, and have approved, new operational modes. Expressed strong conviction of the requirement for commonality, and therefore for a mechanism for achieving it, such as the minimum requirements section.

f. Navy - expressed basic approval for the paper with two major reservations; desired a capability which allows for an intelligence fusion center type of requirement (i.e., essentially a multi-level mode for a controlled environment and limited access capability), and, as discussed above, preferred to have the scope of the document limited to SCI only. The Navy member also noted that the present draft eliminates the collateral mode which presently exists.

STAT

4. The next meeting was set for Tuesday, 20 April at 0930 at the
[   ] McLean VA. Members are asked to come prepared to
discuss the following topics:

- the scope of the DCID; SCI only or all foreign intelligence?

- content of both the general policy and the accompanying
regulation.

- minimum requirements section (i.e., hardware/software, physical,
    personnel, etc.)

- network requirements

STAT

[   ]

Executive Secretary